The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/28/2010

SUBJECT:
Vulnerability in Multiple Adobe Products Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Adobe Flash Player, Reader, and Acrobat that could allow remote code execution. Adobe Reader allows users to view Portable Document Format (PDF) files. Adobe Acrobat offers users additional features such as the ability to create PDF files. Adobe Flash Player is used to view animations and movies using a web browser. This vulnerability can be exploited by opening a malicious Adobe Flash, Reader, or Acrobat file. This file could be sent via email, hosted on a web site, or placed on a network share. Successful exploitation may result in an attacker gaining the same privileges as the logged on user within the scope of the application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

Please note that there is no update available for this vulnerability. There are reports of this vulnerability being actively exploited on the Internet. An update for Adobe Flash Player 10.x for Windows, Macintosh, Linux and Android will be released by November 9, 2010. An update for Adobe Reader and Acrobat 9.4 and earlier 9.x versions will be released during the week of November 15, 2010.

SYSTEMS AFFECTED:
Adobe Flash Player 10.1.85.3 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems
Adobe Flash Player 10.1.95.2 and earlier for Android
Adobe Reader 9.4 and earlier 9.x versions for Windows, Macintosh and UNIX*
Adobe Acrobat 9.4 and earlier 9.x versions for Windows and Macintosh*

*__Note:__ Adobe Reader and Acrobat 8.x are not affected by this vulnerability.

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**
Businesses:
Large and medium business entities: **High**
Small business entities: **High**
Home users: High

DESCRIPTION:
A vulnerability has been discovered in Adobe Flash Player, Reader, and Acrobat that could allow remote code execution due to an issue with the authplay.dll. This vulnerability can be exploited if a user visits a specially crafted web page or opens a malicious Flash Player, Reader, or Acrobat file designed to exploit this vulnerability. Successful exploitation may result in an attacker gaining the same privileges as the logged on user within the scope of the application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

Please note that there is no update available for this vulnerability. There are reports of this vulnerability being actively exploited on the Internet.

RECOMMENDATIONS:
The following actions should be taken:

- For Adobe Reader and Acrobat 9.xconsider deleting, renaming, or removing access to the authplay.dll file that is included with Adobe Reader and Acrobat 9.x. This will eliminate the chance of remote code execution but users will still experience a non-exploitable crash or error message when opening a PDF file that contains Flash (SWF) content.
- Apply appropriate updates provided by Adobe to vulnerable systems as soon as they become available.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:
Adobe:
http://www.adobe.com/support/security/advisories/apsa10-05.html
http://blogs.adobe.com/psirt/

Secunia:
http://secunia.com/advisories/42030

SecurityFocus:
http://www.securityfocus.com/bid/44504

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3654